Microsoft 365 Security Statement of Work

Prepared for Customer

Date: 10/30/2023

|  |  |  |
| --- | --- | --- |
| Architect Name | Account Executive Name | Organization Name |
| Title | Title | Tel (313) 555-0200 Fax (313) 555-0199 |
| architectname@organization.com | accountexecemail@organization.com | organizationwebsite.com |

All information contained in this document is proprietary and is limited to distribution between Organization, Inc. and Customer.

This proposal is valid 60 days from the date shown above.

Table of Contents

Executive Summary 3

Scope of Work 4

Project Deliverables 14

Project Governance 15

Pricing 17

# Executive Summary

<<[ExecutiveSummary]>>

# Scope of Work

## Discovery and Design

### Planning Overview

During Discovery and Design, a Organization Project Manager and Architect will work with the Customer to assemble project teams and develop an overall plan for the engagement.

Immediately after receiving a signed SOW and PO, Organization will begin the process of securing project resources and creating an initial project plan. The Organization Project Manager will have one or more logistics calls with the Customer to define the high-level project schedule and to determine a date and time for the project kick-off call.

#### Activities

* Conduct interviews with technical management, opinion leaders, and staff
* Update the project schedule

### Infrastructure Overview

A Organization Architect will work with the Customer on discovery of the current environment to identify and verify platform readiness. Organization will meet with the Customer to design the tenant to the Customer’s needs through envisioning sessions. These envisioning sessions will cover all technologies in scope for this project. Once all envisioning sessions have been completed and the final design agreed upon, Organization will create the Discovery and Design document for sign-off from the Customer.

#### Activities

* Perform and document discovery of the current environment
* Conduct envisioning sessions for in-scope technologies and document design decisions

**Enablement**

### Microsoft Entra ID 2 Baseline

#### Overview

Microsoft Entra ID plan 2 encompasses the four key features found in plan 1, multi-factor authentication (MFA), Self Service Password Reset (SSPR), Conditional Access, and advanced built-in reporting plus additional security features like Privileged identity management and access reviews. A Organization Consultant will work with the Customer to deploy these features based on the agreed-upon design.

#### Activities

* Configure the following conditional access policies
  + MFA for administrators
  + MFA for users
    - Terms of Use (ToU)
  + Sign-in and User risk profile mitigation policies
* Configure self-service password reset
* Configure group-based licensing
* Privileged Identity Management (PIM)
  + Configure 5 Azure roles for enrollment
    - Global Administrator
    - Compliance Administrator
    - Security Administrator
    - Exchange Administrator
    - SharePoint Administrator
* Access reviews
  + Configure up to 5 access reviews
    - Global Administrator
    - Compliance Administrator
    - Security Administrator
    - Exchange Administrator
    - SharePoint Administrator
* Overview of built-in sign-in and risk profile reports

### Microsoft Purview Information Protection baseline

#### Overview

Microsoft Information Protection (MIP) is a suite of tools and services provided by Microsoft to help organizations protect their sensitive data and maintain data security and compliance. MIP is designed to safeguard sensitive information across various Microsoft applications and services, whether it's stored on-premises or in the cloud.

#### Activities

* Deploy Data classification and Labeling
  + Deploy up to 5 labels to identify documents and data
    - Unrestricted
    - Sensitive
    - Highly Sensitive
    - CUI
  + Configure one basic Microsoft Information Protection policy for all users
* Deploy Data Loss Prevention (DLP)
  + Deploy 2 predefined DLP rules which include sensitive information types
    - ABA Routing Number
    - Credit Card Number
    - US/UK Passport Number
    - US Bank Account Number
    - US Driver License Number
    - US Individual Taxpayer Identification Number (ITIN)
    - US Social Security Number (SSN)
* Configure one email data retention policy based on agreed upon design
* Enable litigation hold for mailboxes currently on hold in source environment

### Defender for Office 365 Baseline

#### Overview

Organization will deploy and configure Defender for Office 365 based on a predefined set of policies developed by Organization Architects.

#### Activities

* Deploy protection policies based on a predefined set of policies
  + Anti-spam
  + Anti-malware
  + Anti-phishing
  + Safe Attachments
  + Safe Links
* Deploy SPF, DKIM and provide DNS records to Customer
* 1 2-hour knowledge transfer session
  + Give an overview of the built-in reporting and analysis options

### Microsoft Defender for Cloud Apps

#### Overview

Software as a Service (SaaS) applications increase flexibility for employees and IT alike. However, they also introduce new challenges and complexities for keeping your organization secure. To get the full benefit of cloud apps and services, an IT team must find the right balance of supporting access while maintaining control to protect critical data.

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across your Microsoft and third-party cloud services.

Microsoft Cloud App Security natively integrates with leading Microsoft solutions and is designed with security professionals in mind. It provides simple deployment, centralized management, and innovative automation capabilities.

#### Activities

* Configure up to 2 of each of the following:
  + Access policy
  + Activity policy
  + App discovery policy
  + Cloud Discovery anomaly detection policy
  + File policy
  + OAuth app policy
  + Session policy
* Configure up to 1 conditional access policy for app control / reverse proxy
* Knowledge transfer for default policies, audit logging, reporting, and Shadow IT functionality
* Configure integrations for the following (where applicable)
  + Defender for Endpoint
  + Defender for Identity
  + Azure AD Identity Protection
  + Microsoft Defender for Cloud (formerly known as Azure Security Center and Azure Defender)

### Defender for Identity

#### Overview

Microsoft Defender for Identity (MDI) is a cloud-based security service which enables analysts to identify, detect and investigate advanced threats directed at your organization. Defender for Identity leverages signals from on-premises Active Directory through sensors deployed on Domain Controllers. Organization will complete the following tasks to deploy Microsoft Defender for Identity.

#### Activities

* Introduce MDI deployment topics: system architecture and features/limitations
* Create MDI instance
* Create group managed service account (gMSA)
* Configure Windows Event collection and SAM-R
* Create honeytoken account
* Install MDI sensors on up to 2 domain controllers and verify healthy sensor status
* Configure alerts, reporting, user roles

### On-premises Azure Active Directory Password Protection for a single forest

#### Overview

#### Activities

* Deploy and configure Azure AD Password Protection proxy service on two domain join, non-Domain Controller, servers
* Deploy Microsoft Azure AD Connect Agent Updater
* Deploy Azure AD Password Protection DC Agent on up to 5 Domain Controllers. It is required that the Customer complete the process to install the agent on all Domain Controllers
* Enable On-premises Azure Active Directory Password Protection in audit only mode
* Develop a custom banned password list, up to 5 entries

Intune

***Overview***

Microsoft Intune is a cloud-based endpoint management solution. Intune provides simplified cloud management for device configuration, device compliance, and app management. Mobile Device Management (MDM) tools, such as Intune, allow administrators to manage and enforce policies on any device that is MDM-aware. Intune also provides Mobile Application Management (MAM) allowing you to provide extra security for your organizational apps and data. MAM can be used with either enrolled or unenrolled iOS and Android devices thus making it especially useful for BYOD scenarios.

***Activities***

* Configure Intune enrollment restrictions
* Configure Azure AD Connect to Hybrid Azure AD Join target Windows 10 devices (as needed)
* Configure and test enrollment methods for targeted platforms
* Enable co-management between Intune and Configuration Manager
* Configure and validate up to 2 device compliance policies per OS platform
* Configure and validate up to 5 device configuration profiles per OS platform
* Configure and validate Windows 10 software update rings
* Create and validate Microsoft 365 Apps for Enterprise application package
* Publish up to 5 applications per OS platform and verify deployment and installation
* Configure and validate iOS and Android App Protection policies
* Configure and validate up to 3 Conditional Access policies
* Configure Role-Based Access Control (RBAC)
* Enroll pilot group of up to 10 Windows 10/11 devices
* Enroll pilot group of up to 10 iOS devices
* Enroll pilot group of up to 10 Android devices

Microsoft Defender for Endpoint

***Overview***

Microsoft Defender for Endpoint (MDE) is a cloud delivered endpoint security solution that provides risk-based vulnerability management and assessment, attack surface reduction, endpoint detection and response (EDR), and advanced hunting capabilities powered by machine learning.

***Activities***

* Develop and implement onboarding procedures for Windows 10/11.
* Review and configure MDE advanced settings
* Review and configure roles and device groups
* For Windows devices, if replacing existing antivirus with Microsoft Defender Antivirus:
  + Deploy antimalware policy to pilot Windows devices
* Deploy Attack Surface Reduction capabilities in audit mode to Windows pilot devices
* Conduct attack simulation: Automated investigation (backdoor)
* Review Microsoft 365 Defender portal

# Project Deliverables

Project deliverables refer to the outputs and results that are produced by the project team. They are critical to the success of the project as they represent the measurable outcomes that the project team and stakeholders are working towards.

To ensure successful delivery of the project, the Discovery and Design document will be required before moving on to Enablement. This ensures the design of the tenant has been agreed upon prior to the start of any configuration and migration of data into the new destination. The period of performance provides the Customer three (3) days to approve or provide feedback on the Discovery and Design document.

Ultimately, the successful delivery of project deliverables is a key factor in achieving project objectives, satisfying stakeholders, and ensuring the overall success of the project.

|  |  |
| --- | --- |
| Phase | Deliverable |
| Discovery and Design | Project schedule  Discovery and Design Document |
| Enablement | As-built document |

# Project Governance

## Project Management

The Project Management Office (PMO) number one goal is to be a center of excellence and own our customer’s project success. Due to the nature of our engagements, our customers require an experienced project manager (PM) who can bring a structured, collaborative, comprehensive, and transparent approach to project management. The Organization PM’s unwavering commitment is to successfully complete projects on time and on budget with clear, constant communication with our customer via workshops, status meetings, and status reports. Organization brings consistent diligence to following established PMBOK processes using our tools and methods towards project planning and management. Our successful record of accomplishment in state and local government, education, and commercial verticals illustrates the level of standard and discipline we will bring to complete your project.

Organization’s methodologies are aligned with industry standards such as PMBOK and ITIL. Project Planning and Management serves as the common thread that brings together multiple stakeholders and resources towards one common goal – enabling our project teams to achieve their full potential to succeed. Organization’s PMs provide the right project management methodology that fits both the type of project and the customer’s needs, whether that be a waterfall or agile approach. Organization has systems in place to support the management of the project for both tasks and collaboration with our customers. Our project teams are ready to begin work on day one and bring a repository of valuable PMO playbooks and tools to drive quick wins and project success. Organization’s PMs provide comprehensive and regular communications to stakeholders to ensure that project goals are being met, risks managed, and issues resolved. Our planning and communication approaches are flexible, scalable, transparent, and provide accountability.

Organization’s project management strategy focuses on core processes: Scope, Schedule, Resource & Budget, Quality, and Risk & Issue management. These processes are interdependent and interact in all project management activities to contribute to project success. Having a defined strategy for management means that Organization is prepared to execute this strategy even before the project kick-off. This sets up the project team for successful project execution!

The Organization Project Management process for this project includes working to develop and manage a project schedule, weekly project status reports, and a weekly status meeting. If at any point it is deemed necessary for more frequent touchpoints this may result in a change order.

## Period of Performance

**The period of performance (PoP) for this project is XX weeks from the project kickoff. This PoP assumes Organization will be “hands on” keyboard which means Organization can do work independently during configuration.** Prior to the end of the PoP, the contract may be amended via change order. Change Orders must indicate the reason for the change and any impact on scope, costs, deliverables, and the period of performance as applicable. If the PoP of the contract is not extended prior to the end date, in order for Organization to continue to provide services, Customer and Organization must agree in writing to a new SOW identifying the terms of the new agreement.

## Resource Plan

To execute the project successfully within the period of performance requires both parties to commit to the resources necessary. Based on our experience, below is the approximate recommended resource commitment needed from the Customer to meet the period of performance. The below recommendations are project resources needed for enablement of this engagement and may not include all parties involved in the project.

### Recommended Customer Role Allocations:

|  |  |
| --- | --- |
| * Project Manager | 30% |
| * Infrastructure / E-mail SME | 30% |
| * Collaboration SME | 30% |
| * Endpoint SME | 30% |

# Pricing

## Fixed Fee Pricing

|  |  |
| --- | --- |
| Milestones | Amount |
| Discovery and Design |  |
| Enablement |  |
| Migration |  |
| Stabilization and Support |  |
| Migration Tools |  |
| TOTAL |  |

Due to the changing nature of cloud services, the pricing above is valid for 60 days from the date of the delivery of this SOW.

## Payment Terms

If included, migration tools will be invoiced up front at project kickoff. This fixed fee contract will be invoiced upon milestone signoff, NET 30 days. Upon notification of milestone completion and a request for milestone signoff, client will have up to 5 business days to provide written conditions of satisfaction if milestone is not complete or to provide the signed acceptance document. If no written notification is received within 5 business days, Organization will assume the milestone is approved and invoice for it accordingly.

Any alterations in the scope will be reviewed with Organization and may result in a change order for additional services and associated costs.

Please make purchase orders out to Organization

Total Contract price shown above for the purchase of goods or services is not inclusive of applicable sales and use taxes. Taxes will be added to invoices when required.

## Travel

Travel is not included in this contract; all work will be performed remotely. Any customer-required travel will be billed at cost.